AO-106 (Rev. 06/09)-Application for Search Warrant

FILED
JUN 26 2023
Mark C. McCartt, Clerk
U.S. DISTRICT COURT

UNITED STATES DISTRICT COURT

for the

Northern District of Oklahoma

In the Matter of the Search of
one Apple iPhone and one Android Cell Phone, Currently Stored at ATF Tulsa Field Office, 125 West 15th St., Ste 600, Tulsa, OK

Case No. 23-MJ-362-CDL

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property one Apple iPhone and one Android Cell Phone, *Currently Stored at* ATF Tulsa Field Office, 125 West 15th St., Ste 600, Tulsa, OK:

See Attachment "A"

located in the Northern District of Oklahoma, there is now concealed one Apple iPhone and one Android Cell Phone:

See Attachment "B"

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. 922(g)	**knowingly possession of a firearm by a prohibited person**
18 U.S.C. 924(c)	**carrying, using, or possessing a firearm in furtherance of a drug trafficking crime**
26 U.S.C. 5861(d)	**possession of an unregistered destructive device**
21 U.S.C. 841(a)(1)	**possession of a controlled substance with intent to distribute**
18 U.S.C. 2312	**Interstate Transportation of a Stolen Motor Vehicle**

The application is based on these facts:

See Affidavit of David Couch, attached hereto.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of ___ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

D Couch
Applicant's signature

David Couch, TFO, ATF
Printed name and title

Subscribed and sworn to by phone.

Date: June 26, 2023

Judge's signature

City and state: Tulsa, Oklahoma

Christine D. Little, U.S. Magistrate Judge
Printed name and title

Affidavit in Support of an Application
Under Rule 41 for a Warrant to Search and Seize

I, David Couch, being first duly sworn under oath, depose and state:

Introduction and Agent Background

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search one Apple iPhone and one Android cellular phone, as further described in Attachment A, for the things described in Attachment B.

2. I am a federal law enforcement officer as defined under Rule 41(a)(2)(C) and am authorized to request this search warrant because I am a government agent who is engaged in enforcing federal criminal laws and I am within the category of officers authorized by the Attorney General to request such a warrant. I am a Task Force Officer (TFO) with the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF). I am currently assigned to the ATF Tulsa Field Office in the Northern Judicial District of Oklahoma, currently assigned to duties in the Northern District of Oklahoma and the Eastern District of Oklahoma. I am an investigative officer, or law enforcement officer, of the United States of America within the meaning of Title 18, United States Code, Section 2510(7), that is an officer of the United States who is empowered by law to conduct investigations of, and make arrests for, offenses enumerated in Title 18. I have been assigned as a TFO since December 2021. Prior to this assignment

I have been an Oklahoma State Trooper for 24 years. During my employment with the Oklahoma Highway Patrol (OHP) I have had assignments in patrol and most recently I am assigned to the Bomb Squad as well as the ATF Task Force. I have conducted and participated in investigations for various criminal cases, to include firearms violations, explosive law violations, bombing and post blast investigations. During my employment with OHP, I have assisted other agencies and law enforcement, including the Drug Enforcement Administration (DEA), and ATF with investigations regarding firearms and narcotics.

3. I am familiar with the facts and circumstances of this investigation. The facts set forth in this affidavit are based on, knowledge obtained from other law enforcement officers, my review of documents related to the investigation, conversations with others who have personal knowledge of the events and circumstances described herein, and review of open-source information including information available on the Internet. Because this affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a search warrant, it does not set forth each and every fact I or others have learned during the course of this investigation.

4. That the following property constitutes evidence of the commission of a criminal offense or that a particular person participated in the commission of the following criminal offenses as defined in United Stated Code 18 U.S.C. 922(g) knowingly possession of a firearm by a prohibited person; 18 U.S.C. 924(c) carrying, using, or possessing a firearm in furtherance of a drug trafficking crime;

26 U.S.C. 5861(d) possession of an unregistered destructive device; 21 U.S.C. 841(a)(1) possession of a controlled substance with intent to distribute; and 18 U.S.C. 2312, Interstate Transportation of a Stolen Motor Vehicle.

5. This affidavit contains only the information I believe is necessary to support probable cause for this application. I have not included every fact or matter observed by me or known to other law enforcement officers. This information is based on my personal knowledge and observations during this investigation, information conveyed to me by other law enforcement officers, and my review of records, documents, and other evidence obtained during this investigation.

Identification of the Device to be Examined

6. The cellular phones to be searched are currently in the possession of ATF Tulsa, 125 W 15th Street Tulsa, OK. The phones are described as an Apple iPhone white in color, IMEI number 356370167372231. One Android cellular phone, model U304AA IMEI number 863382047659428, hereinafter referred to as the devices. The devices were seized form Jason ESSARY, in Vinita, OK on April 29, 2023 during a traffic stop. The Apple iPhone was located in the driver's area of the car and the Android was located in a box within the trunk of the car.

7. The applied-for warrant would authorize the forensic examination of the Device for the purpose of identifying electronically stored data particularly described in Attachment B.

Probable Cause

8. On April 29, 2023, Troopers with the Oklahoma Highway Patrol (OHP) conducted a traffic stop on a reported stolen vehicle. Troopers Seth Hudson and Alex Wilson identified the driver of the stolen vehicle as Jason ESSARY.

9. On April 29, 2023, Oklahoma High Patrol Troopers Seth Hudson and Alex Wilson. Trooper Wilson were patrolling in a marked vehicle on Interstate 44 near mile marker 285 Westbound in Craig County, Oklahoma. Trooper Wilson observed a maroon Chevrolet Camaro, bearing Kansas license plate 351-PYN, entering the westbound toll lane with a large crack in the windshield.

10. Trooper Wilson conducted a vehicle registration check, and the results of the check were that the license plate on the vehicle was previously reported

stolen. Trooper Wilson radioed Trooper Hudson, who also performed a record check and confirmed that the license plate on the vehicle was reported stolen.

11. Subsequently, Troopers Wilson and Hudson initiated a traffic stop of the Camaro. The driver was the sole occupant of the vehicle. The driver was informed of the reason for the stop.

12. When initially approached by the troopers, the driver provided Trooper Hudson a California driver's license with the name "Richard Pilon" and license number #C4229060.

13. Upon review of the vehicle's VIN, Troopers Wilson and Hudson reported the VIN to the OHP Northeast Regional Communication Center (NERCC). NERCC informed the troopers that both the vehicle and the license plate were reported stolen according to the National Criminal Information Center (NCIC) database. NCIC is a national criminal records database that

allows law enforcement agencies to enter or search for information about stolen property, missing or wanting persons, and criminal history.

14. Troopers Wilson and Hudson then informed the driver and placed him under arrest.

15. Because the vehicle was located on a public roadway and reported stolen, the troopers impounded the vehicle. Subsequently, they began an inventory search of the vehicle.

16. During the inventory search, an Apple iPhone (one of the devices) was found in the car near the driver's seat.

17. During the inventory search, WILSON located a metal box on the front passenger seat which contained a large plastic bag containing a white, crystallized substance. Based on WILSON's training and experience, he identified the substance as methamphetamine. Also located in the metal box was a black tar-like substance that is presumed to be heroin, several bags containing marijuana, a bag containing what appeared to be psylocibin (psychedelic mushrooms) several marijuana grinders, digital scale, glass smoking pipes and hypodermic needles. Troopers also located a United States Passport bearing the name Jason ESSARY, photo matched the driver. Troopers then located a wallet and a Missouri

Identification card bearing the name Jason ESSARY. When asked the driver verified that his name was Jason ESSARY.

18. Pursuant to field testing, the white crystallized substance tested positive as methamphetamine, and the black tar-like substance tested positive as heroin. Forensic drug testing by a laboratory is still pending.

19. Several forms of state issued identification were located in the vehicle, including a US Passport and Missouri ID only card bearing the name of JASON MICHAEL ESSARY and two (2) California Driver's License cards bearing the name of RICHARD PILON. Additionally, US currency totaling $9696.00 was located throughout the vehicle and concealed on ESSARY's person.

20. During a subsequent criminal history check of NCIC, it was discovered that ESSARY had several prior felony convictions.

21. Based on my training and experience and the experience of other investigators I know that persons engaged in the illegal sell of narcotics typically carry scales to measure out amounts to be sold and that they deal in large amounts of cash. I also know that the amount of suspected methamphetamine seized, 279 grams, is not typical as to what is possessed simply as a user amount. In my training and experience methamphetamine is typically sold to users in quarter gram, half gram, or one gram amounts.

22. HUDSON located what appeared to be a military surplus training hand grenade inside the passenger compartment. It appeared that the bottom of the

grenade had been drilled through but resealed and there also appeared to be fresh seals around the firing trigger on top of the grenade.

23. While inventorying the property in the trunk of the vehicle, WILSON and HUDSON located five (5) different pistols concealed in different locations throughout the trunk area and one carbine type rifle. An NCIC check revealed that two of the aforementioned firearms had been reported stolen as well.

24. WILSON then located a large-hardened plastic box that he recognized as commonly being used to store weapons, military/law enforcement equipment and other sensitive items in the trunk. The case was removed and opened, at which time WILSON observed a red, white and blue cylinder that had what appeared to be a fuse coming out of one end of it. WILSON also located two (2) vacuum sealed bags inside the case and upon feeling the contents of the bag, WILSON believed that each of the bags contained approximately three (3) additional grenades, similar to the one previously located by HUDSON, each, for a total of seven (7) grenades.

25. Due to the discovery of potential explosive devices, OHP Bomb Squad and a Certified Explosives Expert with the ATF responded to the scene.

26. An initial examination of the grenades by an ATF Explosive Enforcement Officer found that the grenades appeared to be consistent with the

definition of destructive devices under 18 U.S.C. 5845(f). A full report and analysis of the devices by ATF is still pending.

27. Also located in the box was body armor (kevlar type), a portable radio, wireless ear buds for the radio and two additional cell phones that appeared to be "burner phones", multiple high-capacity magazines for a firearm and a large amount of ammunition. One of the phones was an Android smartphone (one of the devices), and the other was an inoperable LG flip phone. [1]

28. In an interview with ATF Special Agent Jon Butler and the affiant, ESSARY confirmed his identity as Jason ESSARY, and admitted to buying the grenades in Missouri and transporting them with him to Oklahoma. ESSARY would not say from whom he had purchased them.

29. During the same interview, ESSARY said that he had previously served two (2) years in prison in California, and more recently served four (4) years in prison.

30. Based on my training and experience and the training and experience of other investigators I know that criminals often use multiple phones or multiple SIM cards for a single phone, and that criminal intelligence is often stored on cellular devices. I know that information, such as photographs and instant messages are stored for long periods of time. I also know that aliases and real identity of unknown persons can be stored on cellular phones. I know that at

[1] One of the phones was an LG flip phone which was powered down and appeared to be completely inoperable. This application does not seek to search that phone.

times firearms are traded for narcotics and that such trades are often communicated and arranged via cellular phones. I also know that pictures are often sent and received of items to be traded or sold.

Technical Terms

31. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where

it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer

software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

f. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

g. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

32. Based on my training, experience, and research, I know that the Device has capabilities that allow it to serve as a wireless telephone, digital camera,

portable media player, GPS navigation device, PDA, and able to access the internet. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

Electronic Storage and Forensic Analysis

33. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

34. I know that cellular telephones are often equipped with digital cameras and those phones possess the capability to transmit and/or store electronic images. I know that in many cases, cellular telephones maintain photographs of illegal activities, including 18 U.S.C. 922(g)(1) Knowing possession of a firearm by a prohibited person, 18 U.S.C. 924(c) Carrying, using, or possessing a firearm in connection with a drug trafficking crime, 18 U.S.C. 842(j) prohibited person possessing explosives affecting interstate commerce, 26 U.S.C.5861 possession of a destructive device without NFA registration, and 21 U.S.C. 841(a)(1) possession of a controlled substance with intent to distribute. These photos are sometimes stored in their cellular phones and often are transmitted or sent from one electronic media device to another. I also know that cellular phones may also contain notes regarding potential illegal acts that are recorded by the subject who possesses the electronics. Furthermore, I know that text messages and emails are

often used by two or more persons to communicate information regarding illegal activities, between principals and co-conspirators of those crimes.

35. I know that cellular telephones are utilized by the majority of individuals in the United States and have become a staple of communication between individuals using text messaging, visual and audible communications (telephone calls and FaceTime type communications) as well as applications like "Whatsapp" and "GroupMe." Additionally, individuals utilize their cellular devices to take pictures, keep notes, as a GPS (global positioning System) device, and even to conduct illicit or illegal activity. Communications on phones are kept for long periods and transferred from one phone to another when replaced. This is done through the use of Cloud storage and direct transfer conducted at the time of purchase or by the individual themselves. Individuals utilize this method as not to lose data that is stored on the phone such as contacts, photos, notes, and other important information to the individual. This data includes contacts used to conduct illegal activities to include; 18 U.S.C. 922(g)(1) Knowing possession of a firearm by a prohibited person, 18 U.S.C. 924(c) Carrying, using, or possessing a firearm in connection with a drug trafficking crime, 18 U.S.C. 842(j) prohibited person possessing explosives affecting interstate commerce, 26 U.S.C.5861 possession of a destructive device without NFA registration, and 21 U.S.C. 841(a)(1) possession of a controlled substance with intent to distribute.

36. Cellular telephones are often used to facilitate offenses and allow criminals to maintain communication with each other before, during and after

the commission of offenses. I am aware that cellular telephones have the capacity to store a vast amount of information, including but not limited to: telephone numbers, voice messages, text messages, e-mail, photographs, videos, address books, records, phone call histories, contact and other information. This information may be contained on the cellular telephone.

37. Based on my training and experience, I know that individuals involved in criminal activity often use cell phones and other electronic devices to further their trade by conducting business on them via text messages and phone calls. Individuals involved in violent crime also trade images of firearms and/or items from their illegal activity on their phone as well. I also know from training and experience that:

a. Cellular telephones are almost always used by persons engaging in criminal activities as a means of communication. They will communicate by verbal conversations, digital text messaging, and/or sending photographs to one another.

b. Persons engaged in criminal activities carry and possess firearms during and in relation to and in furtherance of crimes. They also photograph themselves and others with controlled substances, firearms, and money proceeds. Such photographs are often kept in digital form on cell phones.

c. Cellular telephones may also contain notes, emails, and text messages regarding money laundering, or inquiries for firearm(s) by the subject who possesses the cellular telephone.

d. Text messages and e-mails are often used by two or more persons to communicate information regarding illegal activities between two telephones or between one telephone and a personal computer. This information can include directions for deliveries, stash locations, prices, cell phone contact numbers, and instructions.

e. Cellular telephones often contain stored phone numbers and contact information of individuals that conduct business with other co-conspirators that possess the cellular telephone.

f. Persons prohibited from legally possessing firearms frequently do not obtain firearms by a traditional means (such as through licensed dealers which require background checks and paperwork/documentation) and instead use third-party firearms suppliers. Many of these third-party suppliers are online marketplaces such as Armslist (www.armslist.com) or Gun Broker (www.gunbroker.com), while other third-party transactions take place through the communication between two individuals in a private sale transaction, which takes place outside of the restrictions of the federal government that would at minimum document the sale or transfer.

g. People who have previous felony convictions utilize many methods to obtain firearms. These methods include but are not limited to gun show purchase from private sellers, straw purchasers, stolen firearms, trading firearms for narcotics and stealing firearms. The use of cellular devices is a key way for these individuals to communicate in the movement of illegally

obtained firearms. They utilize the devices to take pictures of firearms, discuss prices, brag about the firearms they have, and talk about the origin of the firearm (if it is stolen or has been involved in other crimes). They also use their phones to order firearms or communicate the type of firearm they would like someone to purchase for them when utilizing a straw purchaser. The phone's internet function can be used to look up firearms as well as dealers in the area that the straw purchaser can buy from, and to access third-party suppliers such as Armslist and Gun Broker. Information about the sale and purchase of firearms is communicated via messaging, which many times include pictures.

h. An additional avenue prohibited persons frequently use to obtain firearms is through the straw purchase of a firearm which is done when a non-prohibited person buys a firearm through traditional means for a prohibited person, at the direction of the non-prohibited person to include style, make, model, and caliber and sometimes even the individual to buy from. Frequently, this communication between the non-prohibited and prohibited person takes place via cellular device to include text messages with both instructions for purchase and pictures of firearms to be obtained.

i. In summary, prohibited persons frequently use cellular phones to obtain their illegally possessed firearms whether it be through third party web sites, private purchase, or through straw purchase.

38. *Forensic evidence*. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored

on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

39. *Nature of examination*. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

40. *Manner of execution*. Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

41. *Methods of examination*. In conducting this examination, law enforcement personnel may use various methods to locate evidence and instrumentalities of the crime(s) under investigation, including but not limited to undertaking a cursory inspection of all information within the Device. This method is analogous to cursorily inspecting all the files in a file cabinet in an office to determine which paper

evidence is subject to seizure. Although law enforcement personnel may use other methods as well, particularly including keyword searches, I know that keyword searches and similar methods are typically inadequate to detect all information subject to seizure. As an initial matter, keyword searches work only for text data, yet many types of files commonly associated with stored cellular device data, such as pictures and videos, do not store as searchable text. Moreover, even as to text data, keyword searches cannot be relied upon to capture all relevant communications associated with a cellular device, as it is impossible to know in advance all of the unique words or phrases investigative subjects will use in their communications. Consequently, often many communications in cellular device data that are relevant to an investigation do not contain any searched keywords.

Conclusion

42. Based on the information above, I submit that there is probable cause for a search warrant authorizing the examination of the Device described in Attachment A to seek the items described in Attachment B.

43. I request to be allowed to share this affidavit and the information obtained from this search with any government agency, to include state and local agencies investigating or aiding in the investigation of this case or related matters, and to disclose those materials as necessary to comply with discovery and disclosure obligations in any prosecutions from this matter.

Respectfully submitted,

David Couch
Task Force Officer
Bureau of Alcohol, Tobacco, Firearms,
and Explosives

Subscribed and sworn to by phone on June 26, 2023.

CHRISTINE D. LITTLE
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to be Searched

The property to be searched is one Apple iPhone, white in color, IMEI number 356370167372231; and one Android cellular phone, model U304AA, IMEI number 863382047659428, hereinafter referred to as the devices. The property is currently located at the ATF office at 125 West 15th Street Tulsa, OK.

This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

Particular Things to be Seized

All records on the Device(s) described in Attachment A that relate to violations of United Stated Code 18 U.S.C. 922(g) knowing possession of a firearm by a prohibited person; 18 U.S.C. 924(c) carrying, using, or possessing a firearm in further of a drug trafficking crime; 26 U.S.C. 5861(d) possession of an unregistered destructive device; 21 U.S.C. 841(a)(1) possession of a controlled substance with intent to distribute; and 18 U.S.C. 2312, Interstate Transportation of a Stolen Motor Vehicle, including:

1. Records relating to communication with others as to the criminal offenses listed above; including incoming and outgoing voice messages; text messages; emails; multimedia messages; applications that serve to allow parties to communicate; all call logs; secondary phone number accounts, including those derived from Skype, Line 2, Google Voice, and other applications that can assign roaming phone numbers; and other Internet-based communication media;
2. Records relating to documentation or memorialization of the criminal offenses listed above, including voice memos, photographs, videos, and other audio and video media, including Exchangeable Image File ("EXIF") data and any other metadata associated with those photos and videos, including device information, geotagging information, and information about the creation date of the audio and video media;

3. Records relating to the planning and execution of the criminal offenses above, including Internet activity, firewall logs, caches, browser history, and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, records of user-typed web addresses, account information, settings, and saved usage information;
4. Application data relating to the criminal offenses listed above;
5. Threatening communications related to the criminal offenses listed above;
6. All bank records, checks, credit card bills, account information, and other financial records.
7. Evidence of user attribution showing who used or owned the Device(s) at the time the things described in this warrant were created, edited, or deleted, such as logs, phone books, saved usernames and passwords, documents, and browsing history;
8. All records and information related to the geolocation of the Device(s) and travel in furtherance of the criminal offense(s) listed above; and
9. All records and information related to the coordination, agreement, collaboration, and concerted effort of and with others to violate the criminal statutes listed above.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been

created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.